Auditing the Windows Network

Bart A. Lewin
Chief Technology Officer
Pinnacle Entertainment, Inc.

CS 3-2

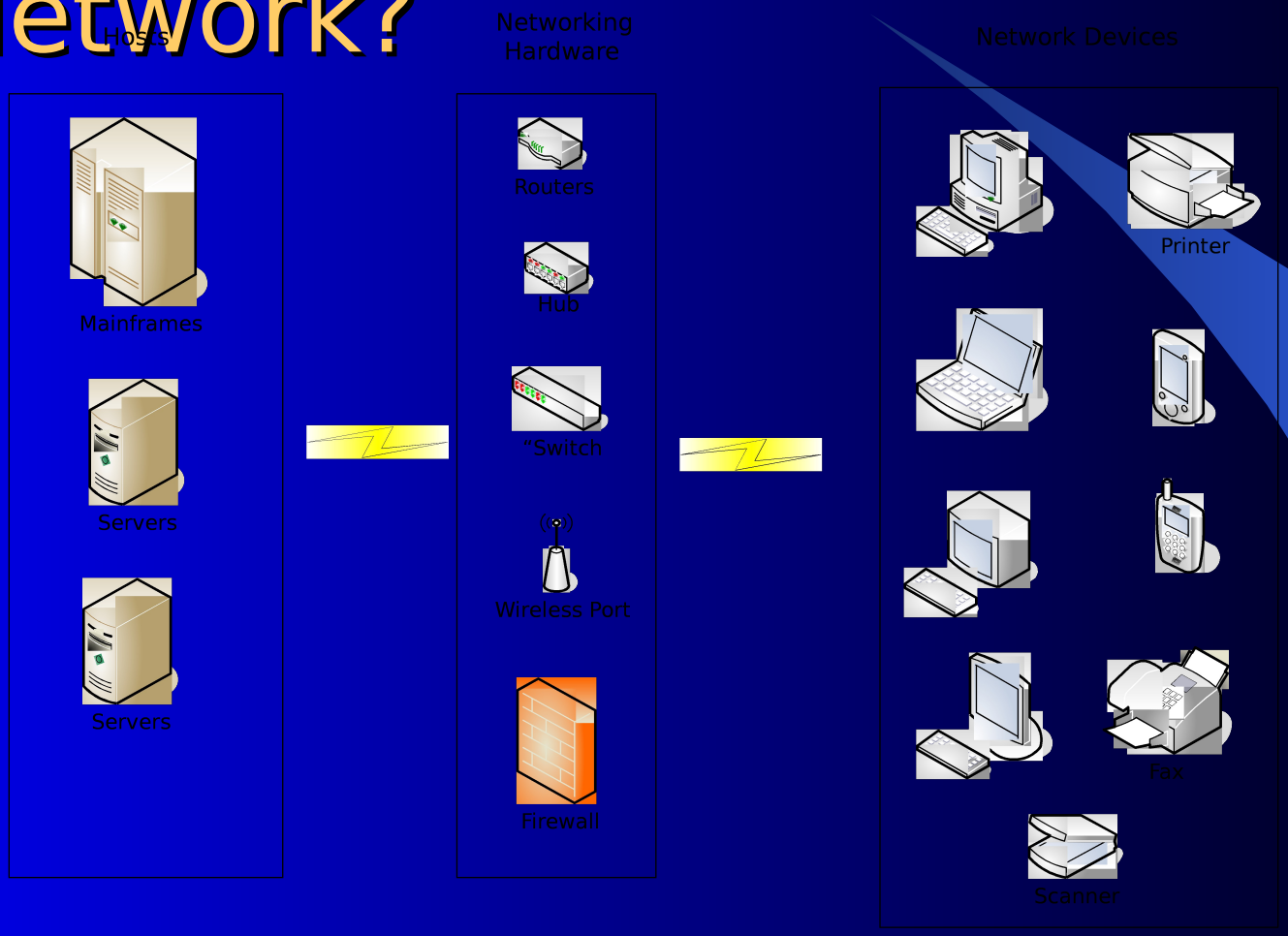
Introduction

- Today, PC based networks contain mission critical applications and data. PC's are also the gateway to applications and data contained on non-PC hosts. Auditing networks is essential to their security.
- Today you will learn the why, how and positive results of network audits.
- But first, let me know a little about you.

Agenda

- Discover the specific reasons why an organization should regularly audit its networks.
  - What is a network?
  - Why should a network be audited?
- Examine the most common techniques used to audit networks, what they uncover, and why.
  - Scanners
  - Blockers
  - Live Intrusion
  - Interviews
- Discuss a case study and examine actual audit results.
- Discuss appropriate remediation for audit findings.

Why Regularly Audit a Network?



Why Regularly Audit a Network?

- What are We Trying to Prevent?
  - Hampered Network Services
    - Viruses
    - Denial of Service Attacks
  - Information Theft
    - Hacking
    - Spyware
    - Trojan Horses, etc.

Why Regularly Audit a Network?

- Why are We Trying to Prevent this?
  - Hampered Network Services
    - Loss of Revenue
    - Loss of Labor Productivity
  - Information Theft
    - Loss of Trade Secrets
    - Loss of other Confidential Business Information
    - Legal Liability

Why Regularly Audit a Network?

- Top Ten Windows System Vulnerabilities from www.sans.org involve:
  - W1 Web Servers & Services
  - W2 Workstation Service
  - W3 Windows Remote Access Services
  - W4 Microsoft SQL Server (MSSQL)
  - W5 Windows Authentication
  - W6 Web Browsers
  - W7 File-Sharing Applications
  - W8 LSAS Exposures
  - W9 Mail Client
  - W10 Instant Messaging

Why Regularly Audit a Network?

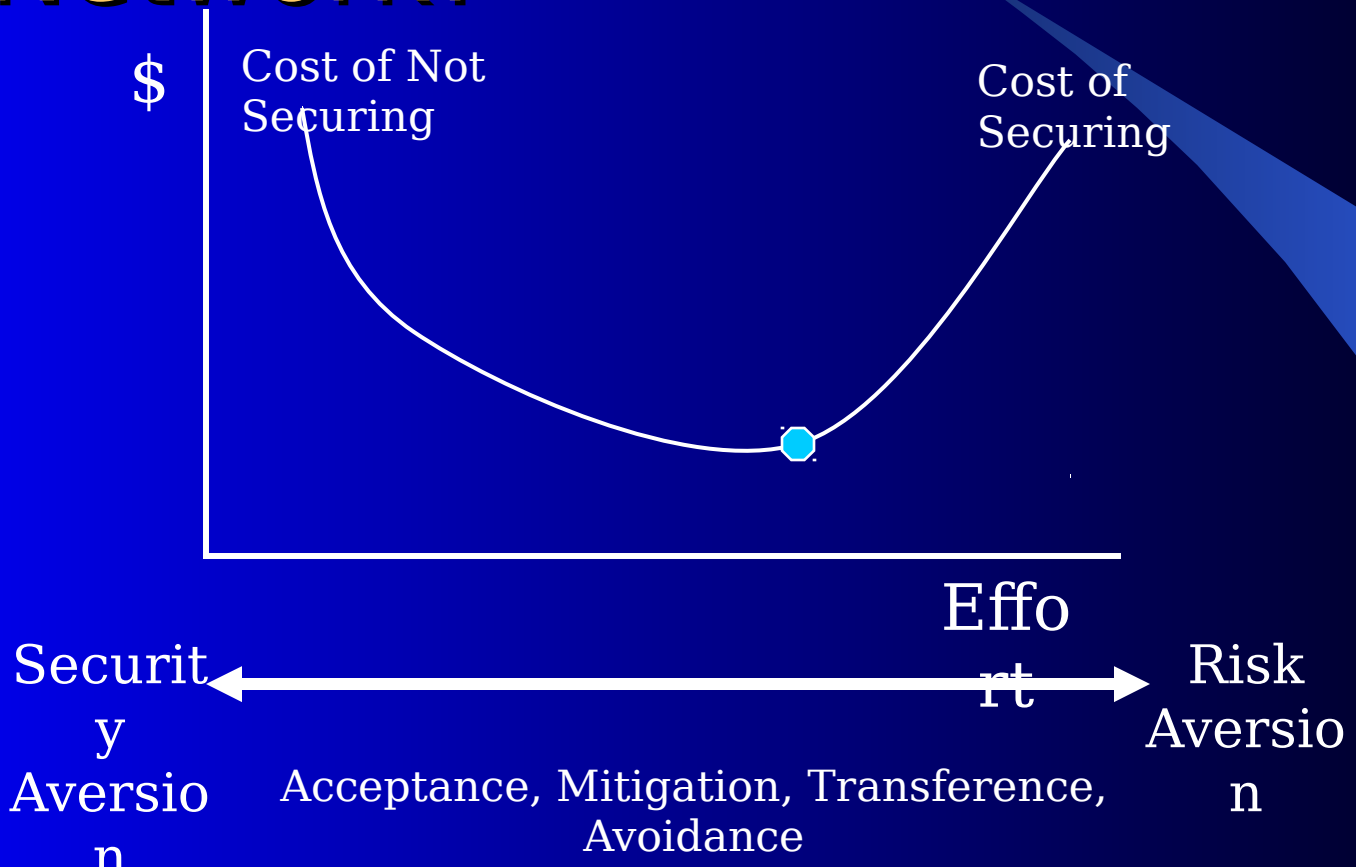


Chart adapted from http://www.theiia.org/eSAC/pdf/BMA_1426.pdf, page 50

Auditing Techniques

- Scanners
  - Security scanners test network nodes for vulnerabilities and report them.
    - Free scanners include Nessus (www.nessus.org) and the Microsoft Baseline Security Analyzers (http://www.microsoft.com).
    - Commercial scanners (i.e., www.eEye.com)
    - Include the ability to automate scans and report variances from stated security policies.
  - Advantage of assisting to preempt attacks.

Auditing Techniques

- Verify Blockers are in Place (Scanners usually do this)
  - Blockers Stop Incoming Threats
    - Include Spam, spyware, trojan horse blockers.
    - Firewalls
  - Prevents known threats, but are little help with unknown threats.

Auditing Techniques

- Live Intrusion
  - Attempting to gain network access information as an outside party confederate.
  - Utilizing from outside the firewalls to attempt to gain access.
  - Assessing the security of physical devices.
  - Assessing the loyalty of employees.

Auditing Techniques

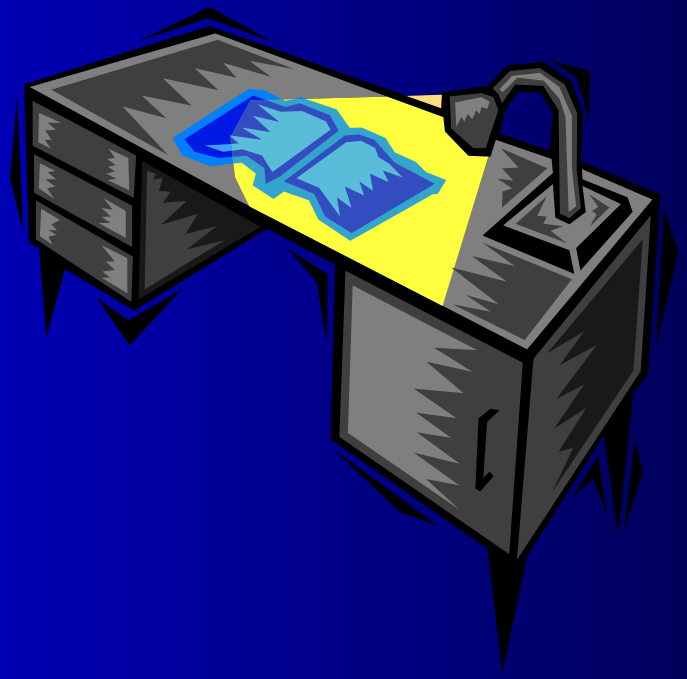
Threats to Information	Occurrence
Laptop Theft	29%
Virus	28%
Insider Abuse of Network	11%
Telecommunications Fraud	6%
Financial Fraud	4%
System Penetration	4%
Theft of Proprietary Information	4%
Unauthorized Insiders	4%
Sabotage	3%
Denial of Service	3%
Telecommunications Eavesdropping	2%
Active Wiretapping	?

Source: http://www.theiia.org/eSAC/pdf/BMA_1426.pdf, page 49

Auditing Techniques

- Interviews
  - Interviewing those responsible for the entry, maintenance and custody of IT systems will assist with:
    - Identifying potential security risks.
    - Identifying the costs of the risk.

Case Study



Remediation

Questions?

Where to Get More Information

- Other training sessions
- List books, articles, electronic sources
- Consulting services, other sources